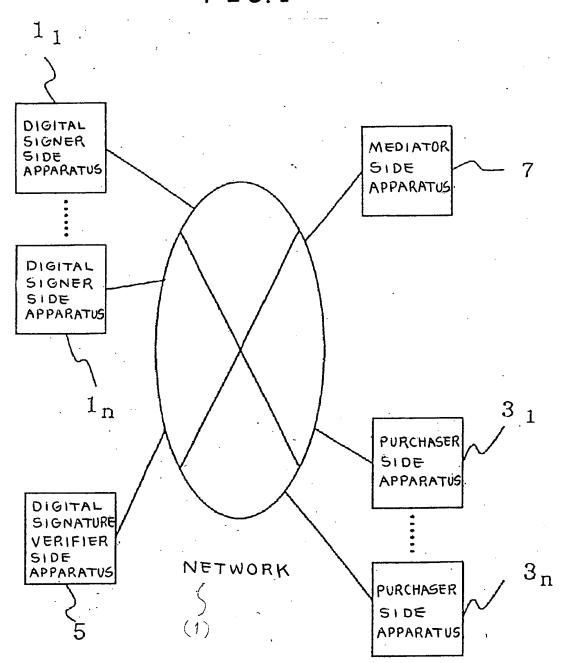
## 国面武 对心符。

【書類名】 図面

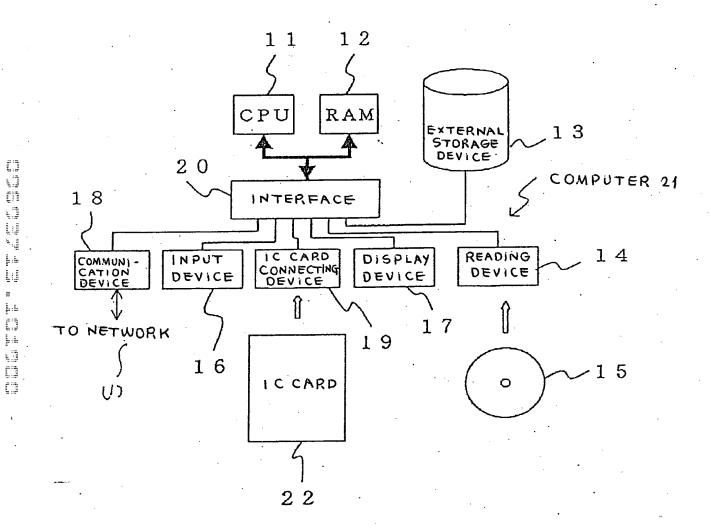
(図1)

FIG. 1



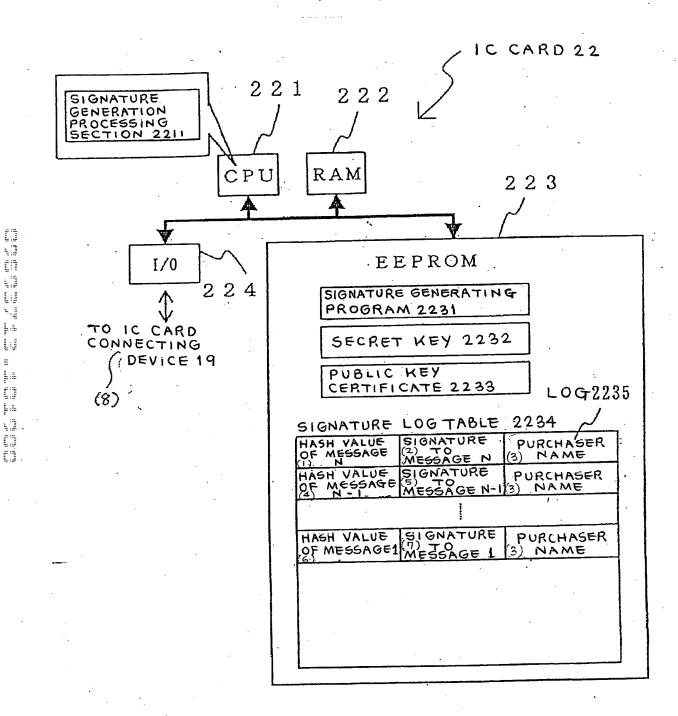
[図2]

F I G. 2



[図3]

F I G. 3



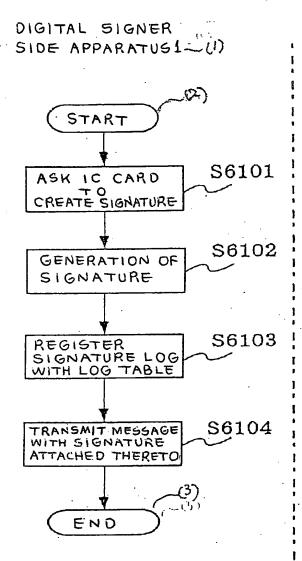
Įij Ē.:ā

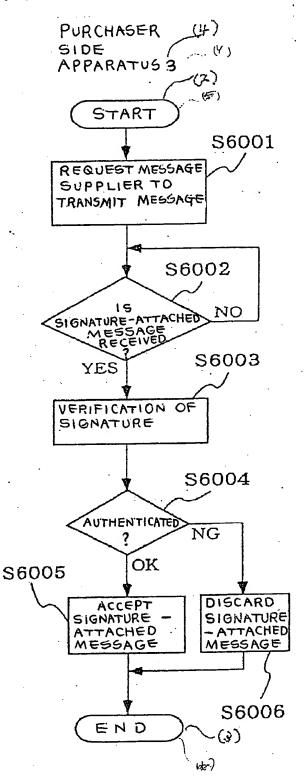
ļ.i.

13

[図4]

F I G. 4





【図5】 FIG. 5 PURCHASER SIDE APPARATUS 3 DIGITAL SIGNATURE DIGITAL SIGNER SIDE VERIFIER SIDE APPARATUSS APPARATUS 1 START START START S7101 S7001 S7201 FIRST - STAGE TRANSMIT SIGNATURE SIGNATURE VERIFICATION REQUEST IS REQUEST VERIFICATION  $\cdot$ NO LOG LIST TRANSMISSION RECEIVED? S7002 S7108 S7102 Y 57202 YES AUTHENTICATED NG ARE VERIFICATION RESULTS RECEIVED AT TROT STAGE TRANSMIT SIGNATURE LOG LIST TRANSMIT OK S7103 NG RESULT YES S7003 S7203 REQUEST TRANSMISSION ARE OUTPUT SIGNATURE LOG VERIFICATION VERIFICATION RESULTS RESULTS NO RECEIVED S7104 S7204 YES NO SIGNATURE LOG LIST RECEIVED END OUTPUT VERIFICATION RESULTS YES S7105 ,(3), SECOND-STAGE SIGNATURE 3) VERIFICATION END S7106. NG AUTHENTICATED SECOND STAGE OK **S7107** TRANSMIT NG RESULT

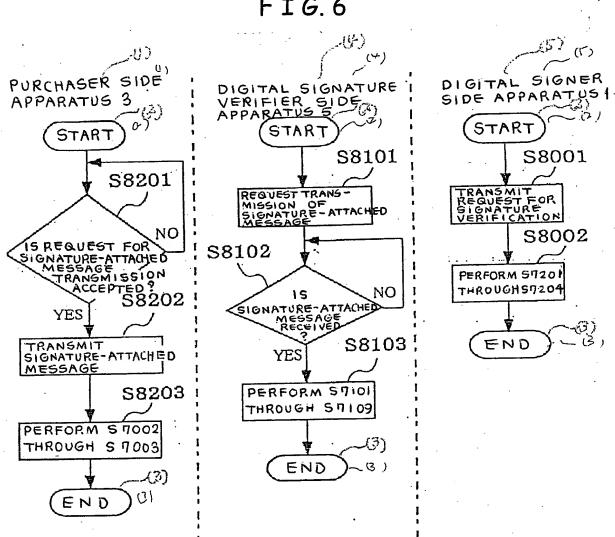
TRANSMIT OK RESULT

END

S7109

【図6】





[図7]

FI6.7

PERCHASER NAME PERCHASER NAME PURCHASER NAME PURCHASER NAME 2235 3 3 £ 3 (12) (12) (12) HASH VALUE h(M.) (13) SIGNATURE SIGN TO SIGNATURE SIGN N-1 TO (PREVIOUS DATA PN-2, PN-13 (9) HASH VALUE h(M2) SIGNATURE SIGN2 TO 0 Signa MESSAGE MI) (PREVIOUS DATA (8) MESSAGE M2) SIGNATURE LOG TABLE 2234 ZX HASH VALUE h (MN) SIGNATURE MESSAGE 3 HÁSH VALUE h(MN-1) OF MESSAGE MN-1 OF MESSAGE MI OF MESSAGE MN. (4)  $\langle S \rangle$  (h(M<sub>N-2</sub>), Sign<sub>N-2</sub>) INITIAL VALUE  $(h(M_{N-1}), Sign_{N-1})$  $P_{N.1}$ DATA P<sub>N-2</sub>  $(h(M_1), Sign_1)$ (1) PREVIOUS (6) PREVIOUS (g) PREVIOUS DATA DATA

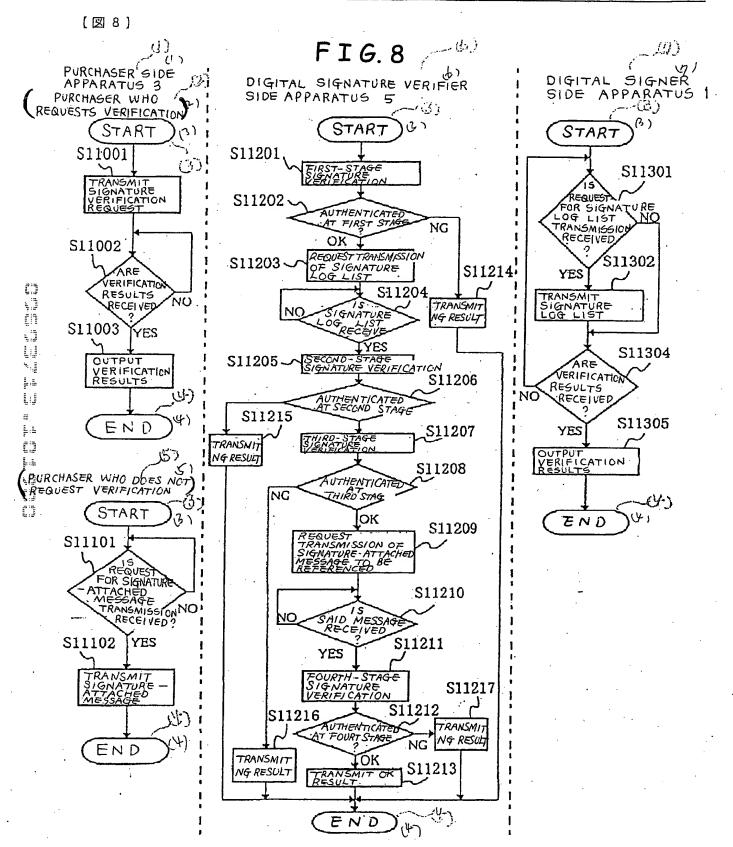
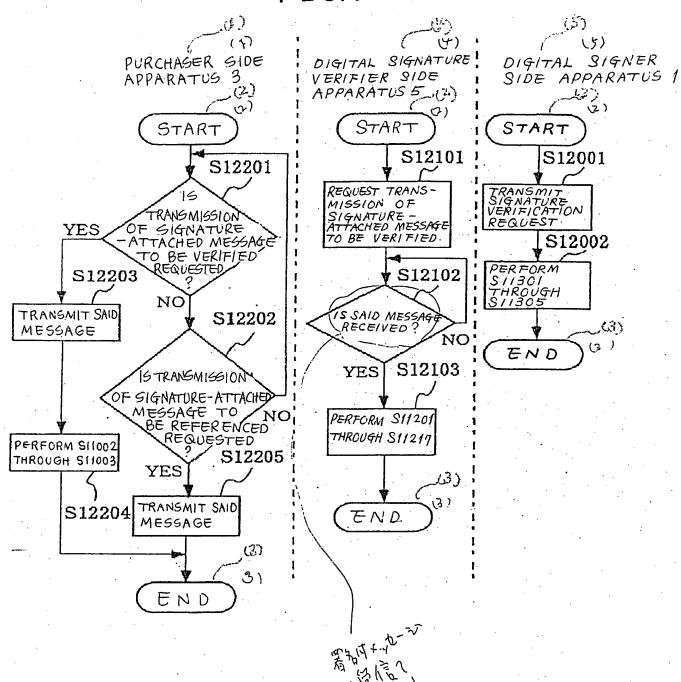
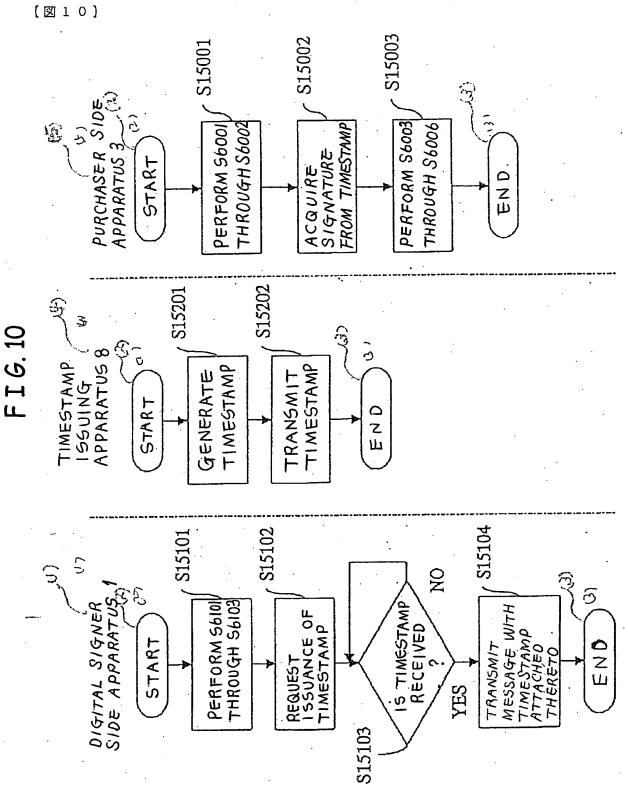
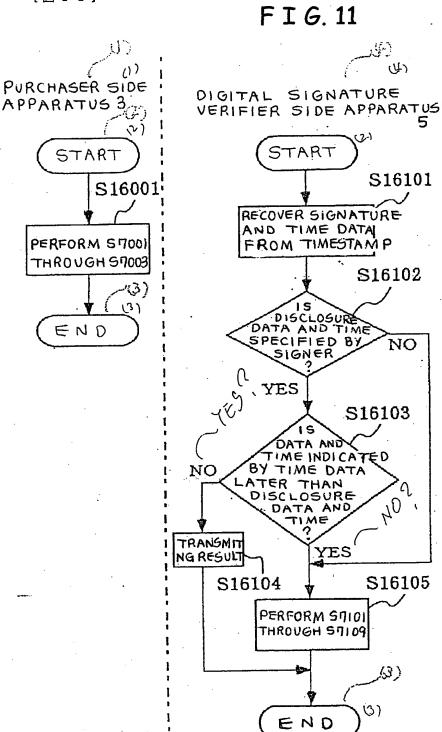


FIG. 9





[図11]



[図12]

## FIG. 12

SIGN	2235 ر		
HASH VALUE OF MESSAGE N	SIGNATURE TO MESSAGE N	B)(3) PURCHASER NAME	TIMESTAMP
び(は) HASH VALUE OF MESSAGE N-1	616) SIGNATURE TO MESSAGE N-1	(3) PURCHASER NAME	NO ENTRY
(8/13) HASH VALUE OF MESSAGE N-m	GIGNATURE TO MESSAGE N-M	(分) PURCHASER NAME	US) TIMESTAMP
MESSAGE N-m-1	SIGNATURE TO MESSAGE N-m-1	(1) PURCHASER NAME	の NO ENTRY・
	•		
HASH VALUE OF MESSAGE 2	(13) (13) SIGNATURE TO MESSAGE 2	DURCHAGER NAME	(7) NO ENTRY
UAN (14) HAGH VALUE OF MESSAGE 1	SIGNATURE TO MESSAGE 1	DURCHASER NAME	ばり TIMESTAMP
-			